## CLAIMS

1. A method for encrypting and decrypting with use of personal cryptoprotective complexes, said method comprising the following steps to be realized in each of the personal cryptoprotective complexes:

a) in a ROM of each of the personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only to said personal cryptoprotective complexes, said way excluding the possibility of copying the mother code to other media and modifying a program code of said programs;

b) connecting, by at least two users, their personal cryptoprotective complexes to a communication link and establishing, by said users, a number of cryptoprotective session participants;

c) producing a random number Z by the personal cryptoprotective complex and storing said number in a random access memory;

d) exchanging, through a communication link, data of the produced random numbers Z between said personal cryptoprotective complexes to establish a time moment of starting the generation of a single-use key of a communication session;

e) synchronous generating a single-use key X of the communication session by reading the stored random number Z out of the random access memory, executing a predetermined arithmetic operation on the random number Z read out of the random access memory and the random number Z' received from another user cryptoprotective device, to derive a resulting number X, and storing the resulting number X in the random access memories;

f) synchronous generating a dynamically transformable daughter code in the individual cyrptoprotective complexes on the basis of the mother code and the single-use key of the communication session;

g) inputting and dividing initial transmitted information into packets of a determined size, and encrypting the packets with use of the dynamically transformable daughter code;

h) transmitting the encrypted packets of information to at least one other personal cryptoprotective complex;

i) receiving the encrypted packets of information in said at least one other personal cryptoprotective complex;

j) decrypting the received encrypted packets with use of the dynamically transformable daughter code;

k) combining the decrypted packets into the initial information, and outputting information to a user;

and repeating steps (f) - (k) to transmit information in a reverse direction during the same communication session.

2. A method according to claim 1, characterized in that the time moment of starting the generation of the single-use key X of the communication session is established according to the moment of transmitting and receiving data corresponding to a last number from said random numbers exchanged through the communication link at the step (d).

3. A method according to claim 1, characterized in that, simultaneously with generation of the single-use key of the communication session, a single-use password of protective-communication-session acknowledgement is generated in each of personal cryptoprotective complexes that coincides at the present participants of the communication session and is used to make sure of establishment of the protected communication session.

4. A method according to claim 1, characterized in that the transformation of the dynamic daughter code at the steps (g) and (j) is synchronized according to the moment of transmitting and receiving of each of information packets.

5. A method according to claim 1, characterized in that in realization of the duplex communication using the personal cryptoprotective complexes, in each of them there are the steps of:

synchronously generating two dynamically transformed daughter codes on the basis of the mother code and the single-use key of the

communication session;

inputting and dividing initial transmitted information into packets of a determined size, and encrypting the packets with use of the dynamically transformable daughter code;

transmitting the encrypted packets of information to at least one other personal cryptoprotective complex;

receiving the encrypted packets of information in said other personal cryptoprotective complex and decrypting the received encrypted packets with use of a second dynamically transformable daughter code;

wherein if the first dynamically transformable daughter code for one of personal cryptoprotective complexes is used for encryption of information, then, said dynamically transformable daughter code for another personal cryptoprotective complex is used for decryption of information and it is accordingly considered to be a second dynamically transformable daughter code;

wherein the transformation of the first dynamically transformable daughter code at the steps (g) and (j) is synchronized according to the moment of transmitting each of information packets, and transformation at the steps (g) and (j) for the second dynamically transformable daughter code is synchronized according to the moment of receiving each of information packets, thus, synchronization of each pair of dynamic transformable daughter codes is carried out irrespective of other pair.

6. A method for encrypting and decrypting information with use of personal cryptoprotective complexes, said method comprising:

in a ROM of each of the personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only to said personal cryptoprotective complexes, said way excluding the possibility of copying the mother code to other media and modifying a program code of said programs; storing an individual number I of the personal cryptoprotective complex in the ROM;

in the personal cryptoprotective complex being a sender of

information:

producing a random number Z and storing said random number in a random access memory,

inputting an individual number I of the personal cryptoprotective complex of an information recipient,

generating a single-use encryption key by reading the stored random number Z and the individual number I out of the random access memory, executing an arithmetic operation on the random number Z and the individual number I to derive a resulting number X, and storing the resulting number X in the random access memory,

generating a dynamically transformable daughter code on the basis of the mother code and the single-use encryption key,

inputting and dividing the sent information into packets of a determined size and encrypting the packets with use of the dynamically transformable daughter code, and

outputting the encrypted packets of information to record onto a medium together with the random number Z to transmit it further to the recipient, wherein the transformation of said dynamic daughter code is made according to the moment of terminating the encryption of a predetermined amount of information bytes;

in the personal cryptoprotective complex being the recipient of information:

reading an individual number I of the personal cryptoprotective complex of the information recipient out of a ROM and storing said individual number in a random access memory,

inputting the number Z received from the information sender to the random access memory,

generating a single-use encryption key by reading the stored random access number Z and the individual number I out of the random access memory, executing an arithmetic operation on the random number Z and the individual number I to derive a resulting random number X, and storing the resulting random number X in the random access memory,

generating the dynamically transformable daughter code on the basis of the mother code and the single-use encryption key,

inputting the encrypted packets of information from a medium, and decrypting the packets by means of said dynamic daughter code, wherein the transformation of said dynamic daughter code is made according to the moment of terminating the decryption of a predetermined amount of information bytes, and

combining the packets and outputting the decrypted information to the information recipient.

7. A method for encrypting and decrypting an electronic document with use of a personal cryptoprotective complex, said method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only to said personal cryptoprotective complexes, said way excluding the possibility of copying the mother code to other media and modifying a program code of said programs; setting date and time in a built-in clock;

in at least one personal cryptoprotective complex being a party of generating an electronic document:

producing, at a command of a user, a decryption password in the form of a random number Y, and a random number Z, deriving a random number Z' or a number I, and storing said numbers in a random access memory;

generating a single-use encryption key X on the basis of said random numbers Z, Z' or the number I read out of the random access memory, and outputting the numbers Z and Y to a user;

generating a dynamically transmittable daughter code on the basis of the mother code and the single-use encryption code;

encrypting a decryption password with use of the dynamically transmittable daughter code;

inputting and dividing initial information into packets of a determined size, and encrypting the packets with use of the dynamically transformable daughter code;

outputting the encrypted packets of information including the encrypted decryption password for transmission together with the numbers Y, Z, Z' and I to personal cryptoprotective complexes of other users or for record to media;

inputting the random numbers Z, Z' or the number I to at least any personal cryptoprotective complex and storing said numbers in the random access memory of the personal cryptoprotective complex, inputting a command to decrypt and inputting the decryption password Y;

generating the encryption password X on the basis of the random numbers Z, Z' or the number I read out of the random access memory;

generating the dynamically transformable daughter code on the basis of the mother code and the single-use decryption key;

inputting the encrypted packets of information, extracting the decryption password from said packets, decrypting said password and comparing it with a decryption password inputted by a user;

in case of coincidence, decrypting the encrypted packets of information, and outputting a decrypted original electronic document to the user, and at non-coincidence, terminating the decryption.

8. A method according to claim 7, characterized in that the step of comparing the decryption password extracted by the user and the inputted decryption password is carried out by encrypting the decryption password inputted by the user in the form of the random number Y with use of the generated dynamically transformable daughter code, and by comparing the encrypted number Y with the decrypted encryption password.

9. A method according to claim 7, characterized in that the random number Z is received from a personal cryptoprotective complex of another user during exchange of the generated random numbers Z through the communication link.

10. A method according to claim 7, characterized in that an

individual number of a personal cryptoprotective complex being one of recipients of the electronic document is used as the number I.

11. A method for encrypting and decrypting an electronic document with use of a personal cryptoprotective complex, said method comprising:

in a ROM of each of the personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only to said personal cryptoprotective complexes, said way excluding the possibility of copying the mother code to other media and modifying a program code of said programs; establishing date and time in a built-in clock;

in one personal cryptoprotective complex generating an electronic document:

producing, at a command of a user, a decryption password in the form of a random number X of a determined digit capacity by a random number generator, storing said number in a random access memory, and outputting it to a user;

generating a single-use encryption key X on the basis of the random number X read out of the random access memory;

generating a dynamically transmittable daughter code on the basis of the mother code and the single-use encryption code;

inputting and dividing initial information into packets of a determined size, and encrypting the packets with use of the dynamically transformable daughter code;

outputting the encrypted packets of information for transmission to personal cryptoprotective complexes of other users or for record to media;

in at least one – any – personal cryptoprotective complex:

inputting a decryption password in the form of a random number X of a determined digit capacity, and a decryption command;

generating a single-use decryption key X on the basis of the random number X read out of the random access memory;

generating a dynamically transformable daughter code on the basis of the mother code and the single-use decryption key;

inputting the encrypted packets of information, decrypting the decryption packets of information, and inputting the decrypted original electronic document to a user.

12. A method according to claim 7 or 11, characterized in that in at least one personal cryptoprotective complex being one of parties generating the electronic document:

a user inputs a command to use the decryption password and inputs any set of symbols via an input device, said set of symbols being assumed to be used as a decryption password and being represented in the form of a number D;

then a random number used as a decryption password is generated by means of the random number generator, and then a determined reversible arithmetic operation between said random number and the number D is carried out to derive finally a number F that is outputted to the user together with the decrypted electronic document for transmission to personal cryptoprotective complexes of other users or for record to a medium;

in at least one – any – personal cryptoprotective complex, inputting the number F there are the steps of: inputting the decryption password D, executing a determined arithmetic operation between said numbers, storing the obtained result in the random access memory of the personal cryptoprotective complex, and using said result to decrypt the inputted information.

13. A method according to claim 7 or 11, characterized in that the step of generating the decryption password comprises: including commands in said password, said commands being addressed to the personal cryptoprotective complexes and establishing the date and time of decryption of the electronic document, wherein the personal cryptoprotective complex of any user who decrypts the electronic document will decrypt it only after the expiration of said date and time; and including predetermined commands

in said password that allow certain modification in the contents of the electronic document.

14. A method according tot claims 1, 6, 7 or 11, characterized in that the step of generating the dynamically transformable daughter code comprises the steps of:

e. 1) reading the number X out of the random access memory, reading a first number M1 of the mother code out of the memory, executing an arithmetic operation on the numbers X and M1 to derive a first resulting number of a determined digit capacity, said resulting number being stored in the random access memory, wherein k low-order digits are separated from said number, and a number corresponding to a determined number of the digit capacity k is assigned to the obtained number P1;

e. 2) reading said first number P1 out of the random access memory, reading a second number M2 of the mother code out of the memory, executing the arithmetic operation on the numbers P1 and M2 to derive a second number P2, and storing said number P2 in the random access memory;

e. 3) repeating step (e. 2) for numbers P(i-l) and Mi, where i = 3, ..., N, for derivation of a set of numbers P3, ..., PN stored in the random access memory;

e. 4) forming two subsets of the set of numbers P1, ..., PN, a first of which consists of numbers corresponding to k low-order digits of numbers P1, ..., PN, and a second set consists of the numbers corresponding to m high-order digits of numbers P1, ..., PN, grouping the second subset of numbers into a table to addresses corresponding to numbers of the first subset, the quantity of said numbers being equal to a possible quantity of numbers in the first subset;

e. 5) selecting a column of the table with a maximum quantity of numbers from the second subset or all columns with an identical maximum quantity of numbers, and executing sequentially the arithmetic operation with consecutive pairs of numbers of selected columns, as a result of which an intermediate number K is obtained;

e. 6) repeating steps (e. 1) - (e. 4) for the number K and the set of numbers P1, ..., PN, wherein step (4) includes selecting k=8 bits and distributing the obtained numbers of the second subset into the table with 256 columns numbered by one of 256 bytes, wherein columns with the quantity of numbers less than two are added by numbers from columns with the maximum quantity of numbers;

e. 7) sequentially executing the arithmetic operation with consecutive pairs of numbers from columns to obtain a number Q1, ..., Q256 of a determined digit capacity for each column,

e. 8) forming two subsets of the set of numbers Q1, ..., Q256, a first of which consists of numbers corresponding to 4 low-order digits of numbers Q1, ..., Q256, and a second set consists of the numbers corresponding to remaining high-order digits of numbers Q1, ..., Q256, grouping the second subset of numbers into a 100x100 table to addresses corresponding to numbers of the first subset;

e. 9) forming a 16x16 table of bytes corresponding to the second subset of numbers from step (e. 8) by consecutive row-wise passing through the 100x100 table, finding cells therein with numbers of said second subset, and recording bytes corresponding to the found numbers into the 16x16 table in the same sequence;

e. 10) executing arithmetic operations on numbers of the second subset from the step (e. 8) corresponding to at least two next bytes for every byte of the 16x16 table to obtain two new subsets and a second 16x16 table, by repeating steps (e. 8) - (e. 9);

e. 11) after the encryption and decryption of a determined amount of information by means of the generated daughter code, updating the first and second 16x16 tables by removal of the first table, its replacement by the second table, and generation of the new second table according to step (e. 10).

15. A method according to claim 14, characterized in that, prior to begin the encryption and decryption of information, there are the following steps in each personal cryptoprotective complex: creating several 16x16

tables in the total amount R by repeating steps (e. 8) - (e. 9), said amount being predetermined and more than two, and storing said tables in the random access memory, wherein an information packet consists of a determined amount of bytes and is encrypted and decrypted using two 16x16 tables, starting with the first and second tables, then encrypting and decrypting a next information packet using the first and third tables and so on up to the last 16x16 table that is also used in a pair with the first table,

then deleting the first table, replacing it with the second table, replacing the second table with the third table and so on up to the last table put on a place of the penultimate table, and putting a new 16x16 table on a place of the last table, said new table being formed according to the step (e. 10), and continuing the encryption and decryption of information packets, starting with the first and second tables.

16. A method according to claim 14, characterized in that the step of generating the dynamically transformable daughter code, starting with step (e. 6), comprises repeating steps (e. 1) - (e. 4) for the number K and the set of numbers P1, ..., PN, wherein step (e. 4) comprises selecting k = 9 bits, and the obtained numbers of the second subset are distributed into a table with 512 columns numbered by one of 512 bytes, while the columns with a quantity of numbers less than two are added by numbers from columns with a maximum quantity of numbers, followed by

e. 7) sequentially executing the arithmetic operation with consecutive pairs of numbers from columns to obtain a number Q1, ..., Q512 of a determined digit capacity for each column,

e. 8) forming two subsets of the set of numbers Q1, ..., Q512, a first of which consists of numbers corresponding to 6 low-order digits of numbers Q1, ..., Q512, and a second set consists of the numbers corresponding to remaining high-order digits of numbers Q1, ..., Q512, grouping the second subset of numbers into a 100x100x100 table to addresses corresponding to numbers of the first subset;

e. 9) forming a 8x8x8 table of bytes corresponding to the second subset of numbers from step (e. 8) by consecutive row-wise passing through

the 100x100x100 table, finding cells therein with numbers of said second subset, and recording bytes corresponding to the found numbers into the 8x8x8 table in the same sequence;

e. 10) executing arithmetic operations on numbers of the second subset from the step (e. 8) corresponding to at least two next bytes for every byte of the 8x8x8 table to obtain two new subsets and a second 8x8x8 table, by repeating steps (e. 8) - (e. 9);

e. 11) after the encryption and decryption of a determined amount of information by means of the generated daughter code, updating the first and second 8x8x8 tables by removal of the first table, its replacement by the second table, and generation of the new second table according to step (e. 10).

17. A method according to claim 14 or 16, characterized by executing the arithmetic operations with numbers by dividing one number by the other and storing the obtained result in the random access memory, followed by selecting n meaning figures in the obtained number which are represented as a natural integer of a digit capacity n, and storing this number instead of a result of division in the memory for further use.

18. A method according to claim 14 or 16, characterized in that the encryption of information is carried out by representing information in 8-bit or 9-bit bytes, respectively, substituting them into the first table, comparing coordinate bytes of initial information in the first table with similar coordinate bytes in the second table, replacing the bytes of initial information by bytes from the second table with said coordinates, and outputting cryptogram bytes obtained as a result of replacement for the subsequent transmission, and decrypting information by replacing the obtained cryptogram bytes by their substitution into the second table, comparing coordinates of the cryptogram bytes in the second table with similar coordinates of bytes in the first table, and replacing cryptogram bytes by bytes from the first table with said coordinates, and outputting bytes obtained as a result of replacement to the user, wherein generation of new tables in encryption and decryption of electronic documents is carried out with taking

into account the electronic documents bytes to be replaced and by means of additional steps using cells engaged in replacement of bytes.

19. A system for realizing a cryptoprotective communication session, comprising a plurality of cryptoprotective complexes each comprising:

a cryptoprotective device including a random number generator, a memory for storing a mother code being a set of random numbers (M1, M2, ..., MN) and being the same for all cryptoprotective devices, a memory for storing encryption, decryption and information processing programs and an individual number of the cryptoprotective device, a microprocessor and a means for protection against non-authorized access to the mother code and programs, said microprocessor and means being coupled to the memory, a non-encrypted information input/output port and an encrypted information input/output port, said ports being coupled to the memory and the microprocessor;

a terminal including a non-encrypted information input/output port and an encrypted information input/output port for connection of the cryptoprotective device, an input device and an output device, said devices being coupled to both input/output ports, at least one port for connection to a communication link, said port being connected to the encrypted information input/output port.

20. A system according to claim 19, characterized in that the terminal further comprises a port for connection to a respective port of a similar terminal of other personal cryptoprotective complex.

21. A personal cryptoprotective complex for cryptographic protection of confidential information, execution of operations with observance of cryptographic protocols, financial operations and electronic transactions, comprising:

a cassette comprising a microchip including a microprocessor capable of suppressing and masking self-microradiations and creating false microradiations, a nonvolatile memory for storing encryption, decryption and information processing programs and an individual number of the cassette, a volatile memory being for storing a mother code and comprising a built-in

accumulator, a protective sheath of the microchip, equipped with a protective sheath integrity monitor unit providing erase of information from the volatile memory at an authorized access from the outside, a non-encrypted information input/output port and an encrypted information input/output port, said ports being coupled to the microchip,

a terminal including a non-encrypted information input/output port and an encrypted information input/output port for connection of the cassette, an input device and an output device, said devices being coupled to both input/output ports, at least one port for connection to a communication link, said port being connected to the encrypted information input/output port,

a user identification device made as an identification wristband, comprising a microchip with a memory for storing access passwords identifying a user, a port for connection to the terminal, said wristband having fixation sensors of latches for automatic turning the microchip on/off for record and removal of the access passwords.

22. A cassette for a personal cryptoprotective complex, intended for protection and storage of confidential and cryptographic information, comprising:

a microchip including a microprocessor capable of suppressing and masking self-microradiations and creating false microradiations,

a nonvolatile memory for storing encryption, decryption and information processing programs and an individual number of a cryptoprotective device,

a volatile memory being for storing a mother code and comprising a built-in accumulator,

a protective sheath of the microchip, connected to the accumulator and a protective sheath integrity monitor unit providing erase of information from the volatile memory at an authorized access from the outside, said protective sheath consisting of three layers wherein the inner and outer layers of the protective sheath are formed with light-reflecting surfaces faced each other, and a third, transparent layer enclosed there between, wherein the light-emitting microdiodes and microphotocells face to the outer light-reflecting

layer, said protective sheath integrity monitor unit being intended to set a periodicity and a radiation doze of the light-emitting microdiodes, to measure power absorbed by the microphotocells, to compare the measured values to reference values, and at their non-coincidence to de-energize the volatile memory for destroying the mother code stored therein.

23. A cassette according to claim 22, characterized in that the microprocessor comprises additional parallel paths to supply signals compensating the microradiations of own signals of the microprocessor, and a generator for generating false microradiations in a frequency band of self-microradiations of the microprocessor.

24. A method of protection against obtrusion of false information with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing an individual number I of the personal cryptoprotective complex in the ROM;

generating a single-use encryption key on the basis of at least one random number produced in said cryptoprotective complex;

generating a dynamically transmittable daughter code on the basis of the mother code and the single-use encryption code, wherein the dynamically transmittable daughter prevents disclosure of the code by a user who knows origin information and its encrypted cryptogram;

inputting initial information and dividing it into packets of a determined size, encrypting each packet for further record to a medium or transmission to other user;

inputting or accordingly receiving the encrypted information to the personal cryptoprotective complex;

generating a single-use decryption key on the basis of said at least one

random number;

generating a dynamically transformable daughter code on the basis of the single-use decryption key and the mother code;

decrypting the received encrypted information, combining packets and outputting the original information to a user, wherein the authenticity of an information encrypting source is established by its decryption using the personal cryptoprotective complex that decrypts only information encrypted with use of a similar personal cryptoprotective complex and with use of the common mother code.

25. A method of protection against obtrusion of false information with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of copying the mother code to other media and modifying a program code of said programs;

storing an individual number I of the personal cryptoprotective complex in the ROM;

generating a single-use encryption key on the basis of at least one random number produced in said cryptoprotective complex;

generating a dynamically transmittable daughter code on the basis of the mother code and the single-use encryption code;

inputting initial information, subjecting it to preprocessing for protection against modification in the encrypted information and authentication thereby of the initial encrypted information, encrypting the preprocessed information for further record to a medium or transmission to other user;

inputting or accordingly receiving the encrypted information to the personal cryptoprotective complex;

generating a single-use encryption key on the basis of at least one random number;

generating a dynamically transmittable daughter code on the basis of the mother code and the single-use encryption code;

decrypting the received encrypted information and authenticating the encrypted information by checking the encrypted information for absence of modification, and outputting the decrypted information to a user only if the result of the check is positive.

26. A method according to claim 25, characterized in that the preprocessing for protection against modification in the encrypted information is carried out by:

a) dividing original information into packets;

b) hashing each packet of initial information with use of a first hash-function and adding an obtained result of the first hashing to the packet;

c) encrypting each packet, including said hashing result;

d) hashing each encrypted packet of information by a second hash-function and adding a second hashing result to the obtained packet for transmission of encrypted packets and the second hashing result to a user or to record them to a medium;

wherein the authenticity of the encrypted information is established by checking the encrypted information for absence of modification as follows:

e) receiving, by a user, the transmitted encrypted packets and the second hashing result. and restoring data partially lost or deformed in data transmission with use of the second hashing result by inverse hashing to obtain at least one variant of the encrypted information packet,

f) decrypting at least one variant of the encrypted information packet, and recording at least one decrypted packet to the random access memory;

g) reverse hashing of decrypted information packets using the first hashing result, and searching for an authentic variant of an initial information packet is carried out, wherein said authentic variant is outputted to the user only upon its detection, and all other decrypted packets are deleted from the random access memory.

27. A method of protection against obtrusion of false information

with use of a personal cryptoprotective complex, said method comprising the following steps to be realized in each of the personal cryptoprotective complexes:

a) in a ROM of each of the personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

b) connecting at least two users with their personal cryptoprotective complexes to a communication link and establishing, by said users, a number of cryptoprotective session participants;

c) producing a random number Z by the personal cryptoprotective complex and storing said number in a random access memory;

d) exchanging, through a communication link, data of the produced random numbers Z between said personal cryptoprotective complexes to establish a time moment of starting the generation of a single-use key of a communication session;

e) synchronous generating a single-use key of the communication session with use of the random number stored in the memory and of a random number received by exchanging data through the communication link;

f) synchronous generating a dynamically transformable daughter code in the individual cyrptoprotective complexes on the basis of the mother code and the single-use key of the communication session;

g) inputting and dividing initial transmitted information into packets of a determined size, and encrypting the packets with use of the dynamically transformable daughter code;

h) transmitting the encrypted packets of information to at least one other

personal cryptoprotective complex;

i) receiving the encrypted packets of information in said at least one other personal cryptoprotective complex;

j) decrypting the received encrypted packets with use of the dynamically transformable daughter code;

k) combining the decrypted packets into the initial information, and outputting information to a user;

said steps (f)-(k) being repeated to transmit information in a reverse direction during the same communication session, wherein protection against obtrusion of false information by repeated use of the encrypted and earlier transmitted information is carried out by using single-use keys of the communication session generated in the personal cryptoprotective complexes on the basis of random numbers one of which is obligatory obtained in each of personal cryptoprotective complexes taking part in protected communications.

28. A method of protection against obtrusion of false information with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing personal data of a user in the ROM, said data including an electronic signature of the user, an individual number of the personal cryptoprotective complex and other attributes to be used for execution of cryptoprotective operations and generation of electronic documents, and establishing date and time in a built-in clock;

in the input of user's information to the personal cryptoprotective complex, inputting user's commands to establish a mode of processing the user's information, to generate an electronic document, and processing the inputted user's information;

in accordance with the established mode of processing the user's information and the earlier received information, generating service information by means of the information processing program, wherein all

service information to be inserted in an electronic document is typical, and combining the service information with the processed user's information to obtain an electronic document, attributes of the electronic document in the form of service information being separated from the processed user's information by means of service symbols that were predetermined in each personal cryptoprotective complex and represent a predetermined set of bits, and if the user uses symbols similar to the service symbols, automatically deleting said used symbols from the user's information in process of its processing before the encryption and excluding thereby obtrusion of false information;

encrypting the electronic document obtained as a result of combining by a dynamically transformable daughter code generated with use of at least one random number, and establishing protection against modification in the encrypted information;

inputting the encrypted information to other personal cryptoprotective complex and making decryption followed by authenticating said information;

searching for service symbols and using them to select the service information located therebetween, inputting user's commands and establishing a mode of processing the decrypted information in accordance with the user's commands, commands derived from the service information, and with earlier inputted information, and outputting the processed information to a user together with service symbols that select and authenticate attributes of the obtained electronic document.

29. A method according to claim 28, characterized by inputting a user's command to sign the electronic document with the electronic digital signature consisting of the personal data of the user, the individual number of the personal cryptoprotective complex, said data and number being earlier inputted to the ROM, and also of a current date and a time of signing the electronic document, and the original information;

generating a decryption password of the electronic document with application of at least one random number, and generating a single-use encryption key based on said password of the present electronic document;

checking the original information for absence of symbols therein similar to service symbols, and if said similar symbols are found, deleting them from the residual initial information;

including information read out from the ROM in structure of the electronic document inputted by the user and having a status of the electronic digital signature of the user, and selecting said information by means of service symbols;

dividing the obtained information into packets of a determined size, encrypting each packet for further record to a medium or transmission to other user;

inputting or accordingly receiving the encrypted information to any personal cryptoprotective complex;

generating a single-use decryption key on the basis of the inputted decryption password of the present electronic document;

generating a dynamically transformable daughter code on the basis of the single-use decryption key and the mother code;

decrypting the received encrypted information, combining packets, outputting the original information to a user, separating the electronic digital signature from the original information by means of service symbols and displaying said electronic digital signature to the user with indication that the present information really is an electronic digital signature exactly of the present electronic document;

using the electronic digital signature to establish the signing date and time and the person who has signed the electronic document, because a registering clerk preliminary puts the user's data present in the electronic digital signature to the ROM of the personal cryptoprotective complex simultaneously with registration of said data in a public database; besides, the electronic digital signature includes an electronic photo of the user that allows identification of the electronic digital signature without reference to the database.

30. A method according to claim 29, characterized by the following steps carried out for registration of the electronic digital signature of the user:

taking the user's data, the individual number of his or her personal cryptoprotective complex, a user statement recorded by a digital video camera and containing information that allows to identify the user;

inputting information to the personal cryptoprotective complex of a registering clerk, signing the received information with an electronic digital signature of the registering clerk, encrypting said information and sending it to a central server;

inputting information to a central cryptoprotective complex, decrypting the received information, putting the decrypted information into a database of electronic digital signatures, generating the electronic digital signature of the user from the received information, certifying said signature by an electronic digital signature of the central cryptoprotective complex containing a predetermined information, encrypting and sending said information to the personal cryptoprotective complex of the user;

receiving and decrypting information in accordance with an incorporated program, checking the electronic digital signature of the user for conformity with a typical template, checking presence of the electronic digital signature of the central cryptoprotective complex, collating an individual number contained in the received electronic digital signature of the user with the individual number of the personal cryptoprotective complex of the user, and in case of positive results, recording the electronic digital signature of the user to the ROM of his or her personal cryptoprotective complex.

31. A method according to claim 29, characterized by signing electronic documents with an electronic digital signature having the status of an electronic seal and containing data of a determined legal person registered in a database, wherein the present electronic signature can be transmitted to a PROM of other personal cryptoprotective complex with simultaneous removal from the PROM from which the transmission has been made.

32. A method for transmission of information with protection against copying with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs, as well as personal data of a user including his or her electronic signature and other attributes used for execution of cryptoprotective operations and generation of electronic documents, and setting date and time in a built-in clock;

in the input of user's information to the personal cryptoprotective complex, inputting user's commands to establish a mode of processing the user's information, to generate a non-copied electronic document, and processing the inputted user's information;

in accordance with the established mode of processing the user's information and the earlier received information, generating service information by means of the information processing program, and combining the service information with the processed user's information to obtain an electronic document, attributes of the electronic document in the form of service information being separated from the processed user's information by means of service symbols, and in accordance with a user's command to generate a non-copied electronic document, including a command in the service information, said command being intended for the personal cryptoprotective complexes and being in the form of a typical set of symbols inputted earlier to the ROM in structure of the information processing program, and storing the obtained electronic document in a section of the ROM intended for non-copied electronic documents of the personal cryptoprotective complex;

establishing a protected communication session with application of the personal cryptoprotective complexes on the basis of a single-use key of the communication session generated using random numbers, and inputting a user's command to transmit the non-copied electronic document recorded in the PROM to other subscriber of the established communication session;

encrypting the electronic document by a dynamically transformable daughter code while reading an electronic document inability-for-copying command out of the service information, establishing the protection against modification to the encrypted information, and transmitting the encrypted information to another personal cryptoprotective complex;

upon termination of transmission of the non-copied electronic document, disabling it for a predetermined time period T1 in the PROM according to said inability-for-copying command;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in said information,

searching for and selecting service information from decrypted information by means of service symbols, using the service symbols to find the service information containing the electronic document inability-for-copying command, recording the electronic document to the section of the PROM intended for non-copied electronic documents, and disabling said document for the predetermined time period T1;

generating an electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of a receiving party and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of a sending party;

in case if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient during the time period T1, enabling the electronic document in the PROM of the personal cryptoprotective complex of the sender, while ignoring the subsequent reception of said password;

in case if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, deleting the electronic document from the PROM of the personal cryptoprotective complex;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending party, generating an electronic-document-transmission-acknowledgement password, and requesting a user acknowledgement in response to the sending of the present password to the personal cryptoprotective complex of the receiving party;

in case if the user gives no acknowledge in response to the sending of the password during a predetermined time period T2, then, on the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user acknowledges the sending of the password during the time period T2, sending the present password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from PROM of the personal cryptoprotective complex of the sender, and said electronic document is automatically enabled in the PROM of the personal cryptoprotective complex of the recipient when he or she has received said electronic-document-transmission-acknowledgement password, followed by inputting user's commands, establishing a mode of processing the decrypted information according to the user's commands received from the service information and according to the earlier inputted information and the information processing program, and outputting the processed information to the user together with service symbols that authenticate attributes of the received electronic document.

33. A method according to claim 32, characterized by receiving decrypted information to the personal cryptoprotective complex, said information being the non-copied electronic document containing a variable face value denoted in a predetermined way by service symbols;

decrypting said information and recording the received electronic document to the ROM of the personal cryptoprotective complex;

determining service symbols in the electronic document by means of the information-processing program;

determining a variable face value information of the electronic document in service information, and outputting said variable face value information to the user;

subdividing the electronic document into arbitrary parts by changing face values of parts using the information processing program in such a manner that their total sum remains invariable, wherein other characteristics and attributes of parts of the electronic document also remain unchangeable;

sending parts of the electronic document to other personal cryptoprotective complexes;

receiving several identical electronic documents with variable face values to the personal cryptoprotective complex and automatically collecting said documents using the information-processing program into a unified electronic document by summing their face values.

34. A method according to claim 33, characterized in that the electronic document with a variable face value is an electronic bank bill of exchange with a predetermined time for repayment, wherein the service information of said bill contains data of a bank drawn the bill, including electronic digital signatures of the bank generated using a personal cryptoprotective complex, data of a user who has received the bill, currency and a face value of the bill as well as a bill repayment date after which the bank will enable a mortgage amount of money left at a user's account that will be transferred ahead of time to any holder of the present electronic bill or its part after reception of the electronic bill to the personal cryptoprotective complex of the bank, identify data of the electronic bill and determine its face value, and if the date of repayment indicated in the bill is not later than a current date, the holder will obtain the sum corresponding to the face value of the presented electronic bill.

35. A method for transmission of information with protection against copying with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing an individual number of the personal cryptoprotective complex as well as other attributes used for execution of cryptoprotective operations in the ROM and setting date and time in a built-in clock;

generating a decryption password on the basis of a random number and recording it to a section of a PROM intended for non-copied decryption passwords and closed for users;

generating a dynamically transformable daughter code on the basis of the mother code and the decryption password;

inputting information, including a computer program, to the personal cryptoprotective complex, and making its encryption using said decryption password;

outputting the encrypted information to a user for record to a medium or for transmission to other user;

inputting a command to transmit the decryption password to other user in process of the protected communication session;

encrypting the decryption password on the basis of a single-use key generated using at least one random number, and outputting said password for transmission;

according to the fact that the decryption password has the status of a non-copied electronic document, upon termination of transmission of the present electronic document, disabling it for a predetermined time period T1 in the PROM;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in said information,

searching for and selecting service information from decrypted

information by means of service symbols, using the service symbols to find the service information containing an electronic document inability-for-copying command, recording the electronic document to the section of the PROM intended for non-copied electronic documents, and disabling said document for the predetermined time period T2;

generating an electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of a receiving party and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of a sending party;

in case if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient during the time period T1, enabling the electronic document in the PROM of the personal cryptoprotective complex of the sender, while ignoring the subsequent reception of said password;

in case if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, deleting the electronic document from the PROM of the personal cryptoprotective complex;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending party, generating an electronic-document-transmission-acknowledgement password, and requesting a user acknowledgement in response to the sending of the present password to the personal cryptoprotective complex of the receiving party;

in case if the user gives no acknowledge in response to the sending of the password during the predetermined time period T2, then, on the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user acknowledges the sending of the password during

the time period T2, sending the present password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from PROM of the personal cryptoprotective complex of the sender, and said electronic document is automatically enabled in the PROM of the personal cryptoprotective complex of the recipient when he or she has received said electronic-document-transmission-acknowledgement password;

then recording the decryption password to the section of the PROM intended for non-copied electronic documents and closed for users of the PROM;

inputting information, including a computer program, to the personal cryptoprotective complex and decryption said information on the basis of the dynamically transformable code generated using the decryption password read out of the PROM;

in case of decryption of a computer program, connecting the personal cryptoprotective complex to a computer, recording a decrypted fragment of the program to a RAM of the personal cryptoprotective complex, executing only a part of operations in a microprocessor of the personal cryptoprotective complex compatible to the computer, while executing another part in the microprocessor of the computer.

36. A method according to claim 35, characterized by further inputting a user's command to limit a validity period of the decryption password in time or quantity of events of use;

including appropriate service commands in the decryption password and selecting them by means of service symbols;

encrypting the received service commands in structure of the decryption password, and outputting them for the further record to a medium or transmission to other user while storing the decryption password in the PROM,

simultaneously disabling the access to the decryption password residuary in the PROM of the personal cryptoprotective complex of the user for a predetermined time interval;

inputting or accordingly receiving the encrypted decryption password with service commands included therein;

selecting service commands by means of service symbols, and executing operations with the present decryption password according to the received commands from the service information, exactly: deleting the decryption password from the memory of the personal cryptoprotective complex after the expiration of time pointed in the service information or after use of the decryption password as much times as indicated in the service information.

37. A method according to claim 35, characterized by inputting a command to transmit the decryption password to other user in an encrypted electronic letter;

adding service information separated by means of service symbols to the decryption password, with the indication of the individual number of the personal cryptoprotective complex of the recipient, and also of date and time after which expiration the recipient of the present decryption password can transmit said password to other users of personal cryptoprotective complexes;

simultaneously, generating an electronic letter in the personal cryptoprotective complex of the sender of the decryption password, said letter including the decryption password with the service information added thereto, with additional indication of the date and time in the form of service information as well, and the personal cryptoprotective complex of the electronic letter recipient will be able to decrypt said message only before the expiration of said date and time, wherein the date and time of decrypting the electronic letter should be indicated earlier than or identical to the date and time indicated in the service information of the decryption password;

encrypting the generated electronic letter with the dynamically transferable code based on the single-use key generated from a random number and the individual number of the personal cryptoprotective complex of the recipient of the present electronic letter, and adding said random number to the encrypted electronic letter;

outputting the encrypted electronic letter and the random number for transmission to the addressee together with information decrypted by means of the decryption password;

recording the encrypted electronic letter containing the decryption password together with the random number to a medium or transmitting said letter through a communication link, and upon termination of transmission, deleting the encryption password from the PROM of the personal cryptoprotective complex of the sender;

receiving the encrypted electronic letter, the random number and the encrypted information;

inputting the random number to the RAM of the personal cryptoprotective complex, and reading the individual number of the personal cryptoprotective complex out of the ROM and recording it to the RAM as well;

generating a single-use key on the basis of the inputted random number and the read-out individual number;

generating the dynamically transformable code on the basis of the single-use key and inputting the encrypted electronic letter to the personal cryptoprotective complex;

decrypting the electronic letter using the dynamically transformable code and recording the decrypted text of the electronic letter to the RAM;

defining service information by means of service symbols, finding the service information with indication of the final date and time of decrypting the electronic letter and collating them with the date and time in the built-in clock, and in case if the final date and time are later than the current date and time, deleting the present electronic letter from the RAM;

finding the decryption password, which includes the date and time after which expiration the decryption password may be transmitted to other users, and recording said decryption password to the section of the PROM of the personal cryptoprotective complex, intended for non-copied decryption passwords and closed for users of the PROM;

inputting information, including a computer program, to the personal

cryptoprotective complex and decrypting said information on the basis of the dynamically transformable code generated using the decryption password read out of the PROM;

after the expiration of date and time pointed in the service information included in the decryption password, deleting the present service information from the PROM, with simultaneous removal of the restriction on the further transmission of the decryption password to other users.

38. A method according to claim 32 or 35, characterized by adding a temporary individual number generated by a random-number generator to the electronic document, and an arbitrary inputted value of the time period T2, said number and value being encrypted together with the electronic document;

inputting a command to transmit the electronic document to other user during the protected communication session or in the encrypted electronic letter;

when the transmission of the present electronic document terminates, disabling said document for a predetermined time period T1 in the PROM of the sender and marking said document with an assigned temporary individual number;

in case of failures in transmission of the electronic document, the sender repeatedly sends the present electronic document with the same accompanying data;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in the information;

searching for and selecting service information from the decrypted information by means of service symbols, using service symbols to find service information containing an electronic document inability-for-copying command and the temporary individual number of the present document; collating said number for presence of a disabled electronic document having the same number in the PROM, and in case if coincidence is absent, recording the electronic document to the section of the PROM intended for

non-copied electronic documents, marking it with the assigned temporary individual number and disabling the electronic document for the predetermined time period T1;

in the personal cryptoprotective complex of the receiving party, generating an electronic-document-loading-acknowledgement password on the basis of a random number, automatically adding said temporary individual number of the present electronic document to said password, recording a password to the PROM, and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of the sending party during the protected communication session or in the encrypted electronic letter;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending party, finding the disabled electronic document in the PROM, said document being marked by number corresponding to a number received with the password, and in case of presence of the disabled electronic document and coincidence of numbers there is the step of generating an electronic-document-transmission-acknowledgement password with use of electronic-document-loading-acknowledgement password, said temporary individual number of the electronic document being automatically included therein;

requesting a user acknowledgement for sending said password to the personal cryptoprotective complex of the receiving party;

in case if the user does not give acknowledgement for sending the password during an arbitrary time period T2 which value was inputted beforehand by the sender in establishment of an electronic document sending mode, then after the expiration of a predetermined period of time there are the steps of: automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender; and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user gives acknowledgement for sending the password during the time period T2, then sending said password in the encrypted form

to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from the PROM of the personal cryptoprotective complex of the sender, and when the recipient has received the electronic-document-transmission-acknowledgement password, there is the step of finding the disabled electronic document and the recorded copy of the electronic-document-loading-acknowledgement password in the PROM of the personal cryptoprotective complex of the recipient, said document and said copy being denoted by number corresponding the number received with the password, and only in case of presence of the disabled electronic document, coincidence of numbers and presence of a direct association between passwords, said electronic document is automatically enabled;

then recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents and closed for users of the PROM, and deleting said temporary individual number;

in case of failures in transmission of the electronic document or acknowledgement passwords, users carry out the backup of transmission.

39. A method according to claim 38, characterized by adding an individual number N1 of the personal cryptoprotective complex where from the electronic-document-transmission-acknowledgement password will be sent, a temporary individual number N2 generated by the random-number generator, and an infinite value T2 of the time period to be inputted by the user, said number and value being encrypted together with the electronic document, to the transmittable electronic document;

inputting a command to transmit the electronic document to other user in process of the protected communication session;

when the transmission of the present electronic document terminates, enabling said document for a predetermined time period T1 in the PROM of the sender and marking said document with said assigned number N2;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of

distortion in information;

searching for and selecting service information from the decrypted information by means of service symbols, using said service symbols to find service information containing an electronic document inability-for-copying command and numbers of said document, recording the electronic document to the section of the PROM intended for non-copied electronic documents, marking said document with its assigned number N2 and disabling the electronic document for the predetermined time period T1;

in the personal cryptoprotective complex of the receiving party, generating the electronic-document-loading-acknowledgement, automatically adding said number N2 of the present electronic document to said password and transmitting the result in the encrypted form to the personal cryptoprotective complex of the sending party during the same or other protected communication session;

receiving the electronic-document-loading-acknowledgement of the electronic document in the personal cryptoprotective complex of the sending party, finding the disabled electronic document in the PROM, said document being marked by number N2 corresponding to the number received with the password, and in case of presence of the disabled electronic document and coincidence of numbers, deleting the present electronic document from the PROM, because the time period T2 is equal to an infinite value;

in the personal cryptoprotective complex whose individual number corresponds to the number N1 assigned to the electronic document, inputting a numerical value corresponding to the number N2 of the electronic document, generating the electronic-document-transmission-acknowledgement password while automatically including therein own individual number corresponding to N1 and the inputted number N2;

sending the present password in the encrypted to the personal cryptoprotective complex of the recipient of the electronic document;

when the personal cryptoprotective complex of the recipient has received the electronic-document-transmission-acknowledgement password in its PROM, finding the disabled electronic document marked by the

number N2 corresponding to the number received with the password, collating the numbers N1 in the electronic document and in the password, and only if coincidence of numbers takes place, automatically enabling said electronic document;

then recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents, and deleting the added numbers N1 and N2.

40. A method according to claim 38, characterized by adding the temporary individual number generated by the random-number generator and an infinite value T2 of the time period, said number and value being encrypted together with the electronic document, to the transmittable electronic document;

inputting a command to generate said electronic-document-transmission-acknowledgement password;

generating an electronic-document-acknowledgement password, assigning a number and a variable face value, if any, thereto, said number and variable face value corresponding to the temporary number and temporary face value of the electronic document;

transmitting the electronic-document-acknowledgement password in the encrypted form during a cryptoprotective communication session to a certain user or keeping said password in own personal cryptoprotective complex;

disabling the electronic document for an arbitrary time period T1 in the PROM of the personal cryptoprotective complex, making copies of the electronic document and transmitting them to other users in process of the cryptoprotective communication session or in an encrypted electronic letter;

after the expiration of the time period T1, deleting the electronic document from the PROM of the sender;

receiving copies of the electronic document, decrypting the electronic document, searching for and selecting service information from the decrypted information by means of service symbols; finding a mark that there is a copy of the electronic document, and a temporary individual

number of the present document, recording the electronic document to the PROM and marking it with the assigned temporary individual number;

receiving the electronic-document-transmission-acknowledgement password to a personal cryptoprotective complex of a user who has received the electronic document copy, finding said electronic document copy marked with the number corresponding to the number received with the password in the PROM, and if the numbers coincide, removing the mark that there is a copy from the electronic document copy, and then recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents and closed for users of the PROM, and deleting said temporary individual number;

after the transmission of said password, deleting it from the PROM in the personal cryptoprotective complex of the sender of the electronic-document-transmission-acknowledgement password, and if a part of the password is transmitted with a variable face value, decreasing a face value of a part of said password residuary in the PROM by the sum equal to the transmitted part.

41. A method of user identification with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing personal data of a user in the ROM, said data including an electronic signature of the user, an individual number of the personal cryptoprotective complex and other attributes to be used for execution of cryptoprotective operations and generation of electronic documents, and establishing date and time in a built-in clock;

in the input of user's information to the personal cryptoprotective complex, inputting user's commands to establish a mode of processing the

user's information, to generate an electronic document and to execute a cryptoprotective operation;

before the execution of cryptoprotective operations, connecting a user identification means to the personal cryptoprotective complex, wherein the memory of said means does not contain information that identifies the user to a moment of connection;

outputting a user identification request to a user;

inputting, by the user, identification data of the user and collating said data with data stored in the memory of said cryptoprotective complex and preliminary inputted by the user;

at the coincidence of the identification data inputted by the user with the data read out of the memory, producing single-use access passwords by a random number generator and simultaneously storing said passwords in the personal cryptoprotective complex and the user identification means capable of deleting the stored single-use access passwords from the memory;

directly before the execution of a cryptoprotective operation requiring execution of the user identification, outputting a user identification request to the user;

connecting the user identification means to the personal cryptoprotective complex and transmitting the single-use access password from the user identification means to the personal cryptoprotective complex with simultaneous removal of the used single-use password from the memory of said identification means;

comparing the obtained single-use access password with the single-used password stored in the memory of the personal cryptoprotective complex, and at the coincidence of the passwords, executing the cryptoprotective operation.

42. A method according to claim 41, characterized in that the user performs self-identification by means of said identification means to make access to certain objects containing electronic locks and preliminary stored single-use access passwords being simultaneously stored in the personal cryptoprotective complex and in the user identification means capable of fast

removing the stored single-use password from the memory, while the user identification is carried out by comparing a single-use access password received from said identification means with a single-use password stored in a memory of an access object, and in case of coincidence of the passwords, the access to the object takes place, wherein the access passwords may be obtained by random numbers generators located in a personal cryptoprotective complex and in an electronic lock of the access object, said generators operating under a similar program and producing identical access passwords.

43. A user identification device made as an identification wristband put on the wrist of a user, comprising a microchip with a memory for storing single-use access passwords identifying the user, a lead with a port for connection to a personal cryptoprotective complex and access objects, fixation sensors of latches for automatic turning the microchip on/off for record of the single-use access passwords and their automatic removal when the wristband is taken off.

44. A device according to claim 43, characterized in that the wristband comprises a wireless interface for interfacing with a wireless data transmission channel.

45. A device according to claim 43, characterized in that the lead intended for connection to the personal cryptoprotective complex simultaneously serves for supplying power to an accumulator of the wristband.

46. A device according to claim 43, characterized in that the wristband is provided with an automatic accumulator replacement device used in connection to a terminal.

47. A method for simultaneously exchanging copy-protected electronic documents among users through a communication link with use of a cryptoprotective complex, comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record

is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing an individual number I of the personal cryptoprotective complex in the ROM as well as personal data of a user including his or her electronic signature and other attributes used for execution of cryptoprotective operations and generation of electronic documents, and setting date and time in a built-in clock;

synchronously generating a single-use encryption key on the basis of random numbers produced in the personal cryptoprotective complexes of users;

synchronously generating dynamically transformable daughter codes on the basis of the mother code and the single-use encryption key in the personal cryptoprotective complexes of users;

inputting initial information to each of the personal cryptoprotective complexes of users; in accordance with an established mode of processing user's information and earlier received information, generating service information by means of the information processing program and combining the service information with the processed user's information to obtain an electronic document, wherein attributes of the electronic document in the form of service information are separated from the processed user's information by means of predetermined service symbols, and in accordance with a user's command to generate a copy-protected electronic document, including a certain command in the service information as a part of the information processing program for the personal cryptoprotective complexes, wherein said command is in the form of a typical set of symbols earlier inputted to the ROM, and storing the obtained electronic document in a section of the PROM provided in the personal cryptoprotective complex and intended for non-copied electronic documents;

in at least one of the personal cryptoprotective complexes, inputting a command for simultaneous exchanging the electronic documents, and sending said command in the form of a signal encrypted by means of the

produced single-use encryption key to other personal cryptoprotective complex;

in each of the personal cryptoprotective complexes, inputting a command to start transmission of the non-copied electronic document recorded in the PROM to other subscriber of the established communication session;

encrypting the electronic document with a dynamically transformable daughter code while reading an electronic document inability-for-copying command out of the service information; establishing protection against modification in the decrypted information and transmitting the encrypted information to other personal cryptoprotective complex;

in accordance with the command for simultaneous exchanging the electronic documents, and upon termination of transmission of the non-copied electronic document, disabling it for a predetermined time period T1 in the PROM of the sender;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in information;

searching for and selecting service information from the decrypted information by means of service symbols, using the service symbols to find service information containing the electronic document inability-for-copying command, recording the electronic document to the section of the PROM intended for non-copied electronic documents, disabling said electronic document for a predetermined time period T1 and outputting the obtained electronic document to the user for acquaintance;

in the personal cryptoprotective complex of the receiving party, generating an electronic-document-loading-acknowledgement password and transmitting said electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of the sending party;

if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient during the time period T1, the

electronic document is enabled in the PROM of the personal cryptoprotective complex of the sender;

if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, deleting the electronic document from the PROM of the personal cryptoprotective complex of the recipient;

receiving the electronic-document-loading-acknowledgement in the personal cryptoprotective complex of sending party, generating an electronic-document-transmission-acknowledgement password and requesting a user acknowledgement to send the present password to the personal cryptoprotective complex of the receiving party;

in case if the user does not acknowledge the sending of the password during a predetermined time period T2, then, after the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user gives the acknowledgement for sending the password during the time period T2, then, sending a predetermined signal in the encrypted form containing information of said acknowledgement to other user, and receiving the similar signal from said user;

after the exchange of acknowledgement signals, making synchronization according the last signal, and from the moment of sending a last bit of said signal from one of personal cryptoprotective complexes and to the moment of according reception thereof in other personal cryptoprotective complex, starting a procedure of a simultaneous exchange of the electronic-document-transmission-acknowledgement passwords in the encrypted form, wherein the reception of a password-containing signal from the opposite party is monitored in each of the personal cryptoprotective complexes, and in case of absence or interruption of said signal, the transmission of own password is stopped;

after the sending of the transmission-acknowledgement password,

automatically deleting said electronic document from the PROM of the personal cryptoprotective complex of the sender, and when the recipient has received the electronic-document-transmission-acknowledgement password, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the recipient.

48. A method according to claim 47, characterized by automatically introducing a time value T to the last acknowledgement signal, said value being different from a current time-reading by a time period t which value is generated by the random-number generator;

sending the present signal to other user, and after the expiration of the signal sending time and before the time T comes, transmitting a random signal generated by the random-number generator;

when the time T comes, automatically stopping transmission of the random signal and starting simultaneous transmission of electronic-document-transmission-acknowledgement passwords in the encrypted form, said random signal and the cryptogram of passwords having identical characteristics.

49. A method according to claim 47, characterized in that users make an exchange of a copy of the electronic document preliminary signed by everyone with his or her own electronic digital signature, and after reception, disabling in the PROM and acquaintance with the received electronic documents, at least one of users inputs a command of simultaneous signing the present electronic document;

a signal in the encrypted form is sent to other user, said signal containing information on simultaneous signing the electronic document and being outputted to the user;

after the exchange of the electronic-document-transmission-acknowledgement passwords, there is the step of automatically signing the electronic documents in each of the personal cryptoprotective complexes with the electronic digital signature of the user.

50. A method according to claim 47, characterized by inputting, in one of the personal cryptoprotective complexes, a command to send an

electronic letter at notice and inputting information, adding a number generated by the random-number generator to the present information, separating said number by means of earlier inputted service symbols and encrypting the information by said number with application of a decryption password;

in accordance with said command, recording the decryption password to the PROM of the personal cryptoprotective complex and marking said passwords with said number;

generating the electronic letter at notice from the inputted encrypted information and the service information added thereto, separated with earlier inputted service symbols, containing the number that corresponds to a number of information and the decryption password, and having a command included therein and indicating that the present information is an electronic letter at notice, outputting a copy of the encrypted electronic letter at notice for record to a medium;

establishing a cryptoprotective communication session with a certain user using the personal cryptoprotective complexes, and transmitting the electronic letter at notice;

receiving information; decrypting the service information, finding the number to be recorded to the PROM, and a command that the received encrypted information is an electronic letter at notice, and outputting the present command to the user;

in accordance with said command and a command inputted by the recipient – to send a notice on reception of said message to the sender, generating the electronic document in the form of a preliminary inputted typical notice sheet, inputting the number to said sheet, said number corresponding to a number of the received information; and signing the present electronic document with an electronic signature of the user, said signature containing the current date and time;

sending a predetermined signal in the encrypted form to other user, said signal containing information that acknowledges presence of the notice;

after the sending and respective reception of said signal, simultaneous

changing the electronic notice sheet for an electronic letter decryption password;

receiving said decryption password to the personal cryptoprotective complex of the recipient, using said password to decrypt information received in the electronic letter at notice and outputting said information to the user;

receiving the electronic document being the notice-of-reception sheet of the electronic letter at notice to the personal cryptoprotective complex of the sender, decrypting said electronic document and inputting it to the user and recording a cryptogram of the notice sheet to the medium.

51. A method according to claim 50, characterized by inputting, in the personal cryptoprotective complex of the sender, a command to send an electronic letter at notice and inputting information, adding a number N generated by the random-number generator to the present information, separating said number by means of earlier inputted service symbols, inputting an individual number I of the personal cyrptoprotective complex of the addressee, producing a random number Z;

based on the inputted number I and the random number Z, encrypting the information, including the added random number N;

in accordance with said command, recording the random number Z to the PROM of the personal cryptoprotective complex and marking it with said random number N;

generating the electronic letter at notice from the inputted encrypted information and service information added thereto, separated with earlier inputted service symbols, containing the number that corresponds to the number N of information, and having a command included therein and indicating that the present information is an electronic letter at notice; outputting a copy of the encrypted electronic letter at notice for record to the medium;

transmitting the electronic letter at notice to a node computer, establishing a cryptoprotective communication session with a node cryptoprotective complex connected to the node computer, transmitting the

random number Z to be stored in the node cryptoprotective complex;

receiving the electronic letter at notice from the node computer to the personal cryptoprotective complex of the addressee, decrypting the service information, finding the number N to be recorded to the PROM, and a command that the received encrypted information is an electronic letter at notice; and outputting the present command to the user;

in accordance with said command and a command inputted by the recipient – to send a notice on reception of said message to the sender, generating the electronic document in the form of a preliminary inputted typical notice sheet, inputting the number N to said sheet, said number corresponding to a number of the received information; and signing the present electronic document with the electronic signature of the user, said signature containing the current date and time;

sending a predetermined signal in the encrypted form to the node cryptoprotective complex via the node computer, said signal containing information that acknowledges presence of the notice;

after the sending and respective reception of said signal, simultaneous changing the electronic notice sheet for the random number Z;

receiving the random number Z to the personal cryptoprotective complex of the recipient, outputting the individual number I of the personal cryptoprotective complex and generating a single-use decryption key of the basis of said numbers;

decrypting information received in the electronic letter at notice and outputting said information to the user;

receiving the electronic document being the notice-of-reception sheet of the electronic letter at notice to the personal cryptoprotective complex of the sender from the node cryptoprotective complex via the node computer, decrypting said electronic document and inputting it to the user and recording a cryptogram of the notice sheet to the medium.

52. A method of converting electronic cash or unlimited electronic bank bills into electronic money of incompatible payment systems with use of a personal cryptoprotective complex, said method comprising:

in a ROM of each of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing personal data of a user in the ROM, said data including an electronic signature of the user and other attributes to be used for execution of cryptoprotective operations and generation of electronic documents, and establishing date and time in a built-in clock;

generating an electronic document in a personal cryptoprotective complex of a bank by means of a program included in structure of the information processing program with application of predetermined service symbols, said document being intended for a certain user and including an electronic banknote signed by band and conditions of the bank in the form of certain commands;

establishing a cryptoprotective communication session between the bank and the user with application of personal cryptoprotective complexes, and transmitting the generated electronic document to the user;

receiving said electronic document to the personal cryptoprotective complex of the user and decrypting the electronic document, determining service symbols, using them to determine commands and the electronic banknote signed by bank, recording the electronic banknote to the PROM of the personal cryptoprotective complex and disabling said banknote till reception of certain commands and conformity with conditions of the bank contained in received commands of the electronic document;

receiving electronic cash or electronic bank bills to the personal cryptoprotective complex of the user, inputting a user's command to enable the electronic banknote signed by bank;

in accordance with the user's command, checking the PROM for presence of electronic cash or electronic bank bills and their conformity with the conditions of the bank in the sum, currency and other attributes;

in case of conformity with the conditions of the bank, disabling the sum of electronic cash or electronic bank bills determined by the present condition and simultaneously enabling the electronic banknote, wherein the sum of disabled electronic cash or bills according to the conditions of the bank may exceed the sum of the electronic banknote;

connecting a medium to the personal cryptoprotective complex of the user by means of a terminal and transmitting the electronic banknote to the present medium;

making a payment transaction by said electronic banknote with use of the present medium;

in the bank, receiving the present electronic banknote, put it into a register, and in case if denomination of the electronic banknote is higher than the sum of payment, refunding change to the medium of the user;

billing the sum of the spent electronic banknote minus change to the bank account of the user from the moment of making the transaction, and simultaneously inputting information of an amount of credit in the form of predetermined commands to the personal cryptoprotective complex of the bank;

connecting the personal cryptoprotective complex of the user to the personal cryptoprotective complex of the bank, establishing a cryptoprotective communication session between them, identifying the personal cryptoprotective complexes and inputting a command for repayment of the credit;

calculating the sum for enabling in accordance with the sum and term of the credit, enabling the sum of electronic cash or electronic bank bills determined by calculation; transmitting the sum necessary for repayment of the credit to the personal cryptoprotective complex of the bank while the residuary part of the enabled sum remains at the order of the user.

53. A method of converting electronic bank bills into electronic money of incompatible payment systems with use of a personal cryptoprotective complex, said method comprising:

in a ROM of each of each of personal cryptoprotective complexes,

storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing an individual number of the personal cryptoprotective complex in the ROM personal data of a user, said data including his or her electronic signature and other attributes to be used for execution of cryptoprotective operations and generation of electronic documents, and establishing date and time in a built-in clock;

generating an electronic document in a personal cryptoprotective complex of a bank by means of a preliminary incorporated program with application of predetermined service symbols, said document being intended for a certain user and including an electronic banknote signed by band and conditions of the bank in the form of certain commands;

establishing a cryptoprotective communication session between the bank and the user with application of personal cryptoprotective complexes, and transmitting the generated electronic document to the user;

receiving said electronic document to the personal cryptoprotective complex of the user and decrypting the electronic document, determining service symbols, using them to determine commands and the electronic banknote signed by bank, recording the electronic banknote to the PROM of the personal cryptoprotective complex and disabling said banknote till reception of certain commands and conformity with conditions of the bank contained in received commands of the electronic document;

receiving electronic bank bills to the personal cryptoprotective complex of the user, inputting a user's command to enable the electronic banknote signed by bank;

in accordance with the user's command, checking the PROM for presence of electronic bank bills and their conformity with the conditions of the bank in the sum, currency and other attributes, reading data of the user to which the electronic bill was addressed, said data including individual

number of the personal cryptoprotective complex of said user;

in the electronic bill is in conformity with the conditions of the bank, then enabling the electronic banknote with simultaneous reduction of a face value of said electronic bill by the sum corresponding to the sum of the electronic banknote, wherein the encrypted information containing the user's data taken from said electronic bill is added to the electronic banknote;

connecting a medium to the personal cryptoprotective complex of the user by means of a terminal and transmitting the electronic banknote to the present medium;

making a payment transaction by said electronic banknote with use of the present medium;

in the bank, receiving the present electronic banknote, decrypting information added thereto; from said information, determining a user account where a mortgage amount on said electronic bill is stored and writing-off a sum from said amount, said sum corresponding to the received electronic banknote; putting the electronic banknote into a register, and if denomination of the electronic banknote is higher than the sum of payment, refunding change to the medium of the user.

54. A method according to claim 53, characterized in that, when the user's data, including the number of the personal cryptoprotective complex of the user and contained in the electronic bill, coincides with similar data in the ROM of the personal cryptoprotective complex of the user, there are the steps of: enabling the electronic banknote including a user account number, with simultaneous reduction of a face value of said electronic bill by the sum corresponding to the sum of the electronic banknote; connecting the medium to the personal cryptoprotective complex of the user by means of the terminal and transmitting the electronic banknote to the present medium without addition of additional data to the electronic banknote;

making a payment transaction by said electronic banknote with use of the present medium;

in the bank, receiving the present electronic banknote; determining

from said banknote a user account where a mortgage amount on said electronic bill is stored and writing-off a sum from said amount, said sum corresponding to the received electronic banknote; putting the electronic banknote into a register, and if denomination of the electronic banknote is higher than the sum of payment, refunding change to the medium of the user.

55. A method for making settlements in electronic cash with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

connecting the personal cryptoprotective complexes to each other directly or with use of a communication channel;

establishing a protected communication session with application of the personal cryptoprotective complexes on the basis of a dynamically transformable daughter code generated using a single-use key obtained with use of random numbers, and inputting a user's command to transfer electronic cash of a certain currency and sum recorded in the PROM to other subscriber of the established communication session;

checking presence of a record in the PROM of the personal cryptoprotective complex 34, said record corresponding in the form and contents to electronic cash of required currency;

if said record present in the PROM, reading out the sum corresponding to electronic cash and collating it with a requested sum;

in case if the requested sum does not exceed the read out sum, outputting a user identification request to a user;

inputting information to the personal cryptoprotective complex and collating it with data stored in the personal cryptoprotective complex and appropriately identifying the user;

in case of coincidence, generating a typical electronic document by

means of the information-processing program inputted earlier, said typical electronic document containing a record of electronic cash in the currency and amount requested by the user;

simultaneously modifying the record of the electronic cash stored in the PROM while reducing its cost by the transferable sum;

encrypting said electronic document by the dynamically transferable daughter code, establishing protection against modification in the encrypted information and transmitting the encrypted information to the personal cryptoprotective complex of the user with which the protected communication session is established;

on the termination of successful transmission of the electronic document, deleting it from the PROM;

receiving the electronic document, decrypting the electronic document, establishing the reliability of information by check for absence of distortions in information, and making a record in the PROM, said record corresponding in the form and contents to the received electronic cash.